한국 사이버테러 방지를 위한 효과적 대응방안

성용은* · 윤병훈**

요 약

이 연구의 목적은 한국의 사이버테러 방지를 위한 효과적인 대응방안을 고찰하는 것이다. 이 연구는 문헌연구 분석의 방법을 사용하였다. 이 연구의 결과를 바탕으로 연구자들은 1) 사이버테러에 대한 효율성을 담보하기 위해 '사이버테러방지법(가칭)' 제정, 2) 사이버테러 관련 실질적 콘트롤타워의 구축, 3) 사이버테러 전문가 양성을 확대 할 것을 제안하였다. 끝으로 이 연구의 한계 및 향후 연구를 위한 제언을 논의하였다.

Effective Response Methods for the Prevention of Cyber-terror in South Korea

Yong-Eun Sung* · Byoung-Hoon Youn**

ABSTRACT

The purpose of this research is to explore the effective response methods for the prevention of cyber-terror in South Korea. This research used an analysis of literature research. From the result of this research, the researchers suggested 1) enactment of the 'Cyber-terror Prevention Act' in order to enhance the effectiveness against cyber-terror; 2) establishment of practical control tower for cyber-terror; 3) expansion of the expert training for cyber-terror. The limitations of this research and the recommendations for future research were discussed at the last part of this research.

Key words : Cybersecurity, Cyber-terror, Cyber-terror Prevention Act, Risk Management, Expert Training

접수일(2016년 3월 2일), 게재확정일(2016년 3월 23일)

* 극동대학교 경찰행정학과 (주저자)
** 경동대학교 경찰학과 (교신저자)

1. 서 론

세계 각국은 자국의 안보 차원에서 테러 및 사이버테러 공격에 대한 경각심이 증가되고 있다. 사이버테러는 정확한 공격주체의 신원파악과 책임소재 규명의 어려움과 함께 막대한 피해유발이라는 측면에서 앞으로 사이버테러는 더욱 증가될 가능성이 높다. 특히 우리나라는 세계유일의 분단국가로 남아있으며, 남북 분단이라는 특수한 상황 하에서 북한으로부터 지속적으로 사이버공격을 받고 있다[20][18][16][17][7][13]

최근 들어 우리나라 사이버안보체계를 위협하는 사건이 계속해서 발생하고 있다. 2012년 3월 20일에 북한 정찰총국에 의해서 KBS, MBC, YTN과 농협, 신한은행 등 국내 주요 방송과 금융 6개사의 전산망이 마비되는 사태가 발생했다. 또한 같은 달 대북보수단체 홈페이지 자료가 삭제되고, YTN계열사 홈페이지 자료서버의 파괴 등 일련의 사이버공격이 연속적으로 발생했다. 당시 주요공격수단은 고난도의 기술을 적용한 국내 전력 및 금융 통신망을 대상으로 이루어졌고, 북한 내부에서 국내 주요 공격 경유지에 수시로 접속한 흔적이 발견되었다. 같은 해 6월 25일에는 청와대와 국무조정실의 홈페이지를 비롯한 주요 정부기관, 정당, 언론사 등 16개 기관의 홈페이지 서버가 멈추거나 접속이 불가능한 상태가 되기도 했다. 현재 우리나라 주요 공공기관 업무의 사이버공간 의존도가 지속적으로 증가하고 있기 때문에 북한 및 제3국의 사이버테러 및 공격의 위협으로 인한 국가사이버 안보에 심각한 위기가 발생될 가능성은 이제 초읽기에 들어가 있는 상태라고 해도 과언이 아니다. 이에 이 연구에서는 우리나라 사이버 안보유지를 위해 사이버테러 방지를 위한 효과적 대응방안을 고찰하고자 한다.

2. 사이버테러의 의의

2.1 사이버테러의 개념

테러(terror)에 대한 법률적 개념은 존재하고 있지 않으며, 「국가대테러활동지침」(대통령훈령 제309호) 제2조 제1호에서 제시된 개념을 통해 법률적 개념을 유추적용할 수 있다. 이 지침에서는 국가 또는 국제기구를 대표하는 자 등의 살해·납치 등 이 지침 내에서 규정하고 있는 9가지 유형에 대해 국가안보 또는 공공의 안전을 위태롭게 할 목적으로 행하는 불법 행위로 정의하고 있다.

사이버테러는 사이버 범죄, 사이버戰, 사이버 정보전 등과 혼용되어 사용되기도 한다. 다만 사이버 범죄, 사이버戰, 그리고 사이버 정보전과 달리 사이버테러가 불특정다수에게 위해를 가한다는 점에서 이들 개념과는 차이가 있다는 견해가 있고[25], 사이버범죄, 사이버戰 등과 사이버테러를 구분하는 기준이 주관적이고 평가적이기 때문에 현실적으로 이들 개념과는 차이가 없어 하나의 포괄적인 현상으로 간주해야 한다는 견해도 있다[16]. 그러나, 사이버테러의 개념 역시 명확한 개념은 존재하고 있지 않다. 현재 사이버테러에 대한 개념으로 볼 수 있는 것은「국가대테러활동지침」제2조 제1항 (마)항에서 컴퓨터 통신망을 이용한 정보조작 및 전산망 파괴를 테러의 한 유형으로 제시하고 있다. 또한 국가정보원 국가사이버안전센터에서 발간한 국가사이버안전메뉴얼(2005)에서는 비슷한 개념으로 사회·정치적 목적을 가진 특정 개인이나 테러집단 또는 적성국 등이 해킹 컴퓨터바이러스의 유포 등 전자적 형태의 공격을 통해 사회기반 시설을 파괴하거나 마비시킴으로서 국가안보를 위협하는 행위로 정의하고 있는 정도이다.「국가대테러활동지침」이나 국가사이버안전메뉴얼에서 제시한 개념정의 역시 사이버테러에 대한 명확한 정의는 아니지만, 가장 근접한 개념으로 볼 수 있다. 이러한 내용을 바탕으로 사이버테러의 개념을 정의하면, 소프트웨어와 네트워크를 이용하여 사이버공간에서 테러라는 불법적 행위를 자행하는 것으로 정의가 가능하다[17].

2.2 사이버테러의 유형 및 발생현황

2.2.1 사이버테러의 유형

사이버테러의 유형은 수단과 수법, 그리고 피해를 중심으로 분류하고 있는데, 먼저 경찰청 사이버테러대응센터와 국가정보원 국가사이버안전센터에서 제시한 유형분류를 들 수 있다[4].

경찰청 사이버테러대응센터에서는 사이버테러의 주요 유형을 해킹(단순침입, 사용자도용, 파일삭제 또는 자료유출, 폭탄메일 등)과 악성프로그램(트로이 목

마, 인터넷 웜, 스파이웨어 등)의 유포 등으로 구분한다. 국가정보원 국가사이버안전센터에서는 사이버테러의 주요 유형을 국가기밀에 대한 공격, 반국가단체 및 테러단체 등에 의한 공격, 국가안전보장과 관련된 통신기반시설에 대한 공격, 국가핵심기술 시설에 대한 공격 등으로 분류하고 있다. 이 외에도 전자파일 또는 다양한 자료를 손상, 파괴하거나 변경하는 형태의 정보공격, 하드웨어의 손상, 운영 플렛폼이나 프로그래밍을 와해하여 기능을 마비시키는 형태의 기반시설의 공격, 사이버 상의 커뮤니케이션을 이용하여 보다 사이버 테러를 용이하도록 유도하는 형태의 기술적 조장, 그리고 테러단체의 이념홍보나 기금 마련 등의 유형으로 구분하기도 한다[26][24][17].

2.2.2 사이버테러의 발생현황

사이버테러의 개념과 그 유형이 명확하지 않은 상황에서 발생현황의 범위를 제시하는 것에는 한계가 있지만, 사이버테러형의 범주로 구분하여 현황을 제시한 경찰청의 국회정보공개 자료를 바탕으로 2011년부터 2015년까지 국내 사이버테러의 발생현황을 살펴보면 <표 1>, <표 2>에서 보는 바와 같다. <표 1>은 2011년부터 2013년의 경우 사이버테러형 범죄를 상위 카테고리로 하여 해킹, 바이러스 등의 발생현황을 제시하고 있다. 그러나 2014년부터는 사이버테러형 범죄가 아닌 정보통신망침해 범죄라는 新범죄 유형으로 명칭을 변경하여 해킹, DDos등, 악성 프로그램, 기타 등의 발생현황을 집계하고 있다[27].

2011년부터 2013년까지 국내에 발생한 사이버테러형 범죄를 살펴보면(<표 1> 참조), 2011년의 경우 전체 13,396건 중 해킹이 98.9%(13,253건), 바이러스 유포가 1.1%(143건)로 나타났고, 2012년의 경우 전체 9,607건 중 해킹 99.5%(9,561건), 바이러스 유포 0.5%(46건) 였다. 이듬해인 2013년은 전체 10,407건 중 해킹 98.3%(10,236건), 바이러스 유포가 1.7%(171건)로 발생되었다. 전체적으로 바이러스 유포 보다 해킹에 의한 사이버테러형 범죄가 많이 발생하는 것을 알 수 있으나 2013년에는 전년도 보다 사이버테러형 범죄 중 바이러스 유포의 비율이 3배 가까이 증가한 것을 알 수 있다.

<표 1> 국내 사이버테러 발생현황

(단위: 건)

연도 \ 유형		사이버테러형		
		소 계	해 킹	바이러스
'11	발생	13,396	13,253	143
'12	발생	9,607	9,561	46
'13	발생	10,407	10,236	171

2014년-2015년까지 정보통신망침해 범죄로 사이버테러 유형의 구체적 현황을 보면(<표 2> 참조), 2014년은 전체 2,291건 중 해킹 71.9%(1,648건)로 가장 많았고, 기타 21.3%(487건), 악성 프로그램 유포 5.7%(130건), DDos등 1.1%(26건)의 순으로 확인되었다. 2015년은 전체 1,755건 중 해킹 72.5%(1,273건)로 가장 많았고, 기타 20.3%(356건), 악성 프로그램 유포 6.2%(108건), DDos등 1,0%(18건)의 순으로 나타났다.

<표 2> 국내 정보통신망침해 범죄 발생현황

(단위: 건)

연도 \ 유형		정보통신망침해범죄				
		소계	해킹	DDoS 등	악성 프로그램	기타
'14	발생	2,291	1,648	26	130	487
'15.7	발생	1,755	1,273	18	108	356

2014년과 2015년에 정보통신망침해 범죄라는 新범죄유형 카테고리로 분류한 이후 전체 발생현황이 2011년부터 2013년까지의 사이버테러범죄 발생현황보다 현저히 적은 것을 알 수 있다. 이러한 현상은 국내에 사이버테러의 형태로 발생되는 범죄가 감소한 것이기보다 사이버범죄와 관련된 범죄 유형이 보다 세분화된 결과로 보여지지만, 2013년과 2014년 해킹 발생건수만 보다라도 9,561건에서 1,648건으로 절대적인 해킹 범죄건수 자체가 감소했다고 보기에는 무리가 따른다. 따라서 형사사법기관에서 집계되는 사이버테러 공식통계의 정확성과 신뢰성이 확보되기 위해서 우선 사이버테러의 개념과 그 유형이 명확하게 법률로 정립되어야 하며, 사이버테러 탐지 및 수사기능을 강화해야 할 것이다.

3. 사이버테러의 방지를 위한 효과적 대응방안

3.1 사이버테러 방지 관련 단일 법률 제정

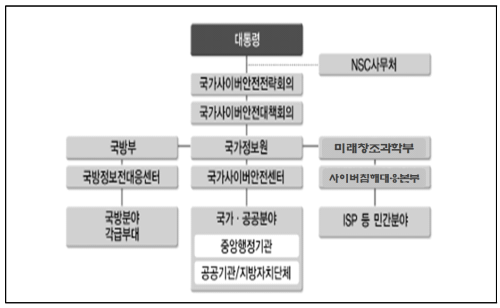
우리나라에서 사이버테러에 대응할 수 있는 법률로는 「형법」, 「정보통신기반보호법」, 「정보통신 이용 및 정보보호 등에 관한 법률」, 「국가정보화기본법」, 「전자정부법」, 「전자서명법」 등 기본법과 특별법 등이 산재되어 있다[19]. 이처럼 사이버테러에 대한 적용 법률이 산재되어 있기 때문에, 사이버테러 발생 시 대응방안 역시 효율성과 신속성이 저하된다. 즉 사이버테러 방지를 위한 단일 법률은 없고, 단지 대통령 훈령인 '국가사이버안전관리규정'만이 존재하고 있는 실정이다. 그러나 '국가사이버안전관리규정'은 대통령 훈령으로써 행정기관 내부에만 효력이 있다는 점에서 국가 전반에 효력을 미치는 데는 한계가 있다. 이에 국회에서는 2006년 공성진 의원등의 안(이하 공성진 의원안)을 시작으로, 하태정 의원등의 안(이하 하태정 의원안), 서상기 의원등의 안(이하 서상기 의원안), 이노근 의원등의 안(이하 이노근 의원안) 등 4개의 안이 입법발의 되었지만, 공성진 의원안의 경우 임기만료폐기되었고, 하태정, 서상기, 이노근 의원안은 아직 국회 계류 중이다.

임기만료폐기 및 계류 중인 법안은 크게 사이버테러의 개념, 사이버테러 관련 컨트롤타워 역할의 주체, 사이버테러 방지 및 위기관리에 대한 책임기관, 사이버위기의 대응훈련 및 위기경보의 주체에 대해 다루고 있다[2]. 요약하자면, 사이버테러의 개념에 대해서는 관련 입법안들이 모두 명확한 개념을 제시하지 못했다는 한계를 지니고 있고, 컨트롤타워에 대해서는 국무총리 소속으로 위원회를 두는 형식과 국가정보원장 소속 하 위원회를 두는 형식을 취하는 2가지 案이 제시되고 있다. 사이버테러 방지 및 위기관리의 책임기관 범위에 관해서는 국가기관 및 공공기관에 국한되어야 한다는 입법안과 민간분야와 기업에까지 확장시켜야 한다는 입법안이 상충하고 있다. 끝으로, 사이버위기에 대한 경보발령주체에 있어서는 공공기관에 대한 발령권자는 국가정보원장으로 규정하고 있다. 이처럼, 단일 법률안의 제정이 필요성하기 때문에 국회에서 꾸준히 입안이 되고는 있지만, 그 세부 내용에 대해서는 다소 입장차가 존재한다.

사이버테러에 대해 효율성 및 신속성을 바탕으로 국가 전반에 효력을 미칠 수 있고, 기관 간 업무의 중복성 해결을 통해 책임소재를 명확히 할 수 있기 위해서는 단일 법률인 '사이버테러방지법(가칭)' 내 법안 간 쟁점에 대해 국가안보적 입장에서 여야(與野)간 조속한 합의를 통해 신속히 제정되어야 한다[2][15][1][5][14].

3.2 사이버테러 관련 실질적 콘트롤타워 구축

현 국가사이버 안전관리체계를 보면(<그림 1> 참조)[22], 국가정보원장을 의장으로 하는 국가사이버안전전략회의의 구성과 국가정보원 차장을 의장으로 하는 국가사이버안전대책회의의 구성 등을 바탕으로 형식적으로는 국가정보원이 국가사이버안전과 관련된 정책 및 관리의 컨트롤타워 역할을 하는 것으로 보여진다. 그리고 국방 분야의 사이버안전과 관련해서는 국방부 산하 사이버사령부에서 임무를 수행하고 있다. 민간영역에서의 사이버안전에 대해서는 박근혜 정부 출범 이후 신설된 미래창조과학부에서 관리하고 있다. 구체적으로는 미래창조과학부 산하 인터넷진흥원(KISA) 내 인터넷침해대응센터를 통해 민간분야의 사이버안전 업무를 수행하고 있는 형태를 취하고 있다. 그러나 미래창조과학부는 조직 신설과정에서 많은 업무들이 이관되었는데, 특히 ICT와 관련된 업무가 그것이다. 이처럼 미래창조과학부는 민간분야의 사이버안전과 관련하여 주무기관으로 부상하게 되었다. 그러나 이관된 업무들의 범위가 명확하게 구분된 것이 아니기 때문에 관련 부처간 주도권 다툼이 발생될 우려 역시 상존하고 있다[21].



<그림 1> 국가 사이버 안전관리체계

<그림 1>에서 보는 바와 같이, 국가정보원이 컨트롤타워 역할을 하는 것처럼 보이고, 실제 3·20 DDos 공격시 국가정보원 주도로 대응팀이 마련되기도 하였지만, 대응팀이 유관기관들과 민·군·관과 협력하기 어려웠다는 문제점이 도출되기도 하였다. 즉, 현 국가사이버안전관리체계에 있어 대응체계는 형식적인 것에 불과하다고 볼 수 있다[1]. 이에 사이버테러와 관련하여 실질적인 컨트롤타워 신설이 필요하다는 인식에는 이견이 없지만, 컨트롤타워의 주체가 국민안전처가 되어야 한다는 입장[8], 국가정보원이 주체가 되어야 한다는 입장[6], 그리고 청와대가 주체[1]가 되어야 한다는 의견들이 존재한다. 생각건대 실질적으로 민·관의 협력 및 공조 등을 이끌어내고 부처간 경쟁이나 다툼을 최소화하기 위해서는 청와대가 컨트롤타워 역할을 하고 국가정보원이 실무를 총괄하는 것이 바람직하다. 그러한 점에서 볼 때, 국가사이버안전전략회의에서 사이버안보 수석이 컨트롤타워를 맡도록 논의된 것은 매우 긍정적이다.

3.3 사이버테러의 효과적 대응을 위한 전문가 양성 확대

사이버테러에 대한 효과적 대응을 위해 전문가 양성 즉, 장기적인 인력수급 정책을 마련해야 하는데 구체적으로는 3가지 정도가 논의된다.

첫째, 사이버테러 대응을 위한 전문가 양성의 법적 근거의 제정이다. 현재, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」과 「정보통신기반보호법」에서는 정보보호 인력 양성에 대한 근거를 제시하고 있지만, 이러한 법적 근거가 사이버안보 혹은 테러 방지에 초점을 두고 있다고 보기에는 다소 한계가 따른다. 이에, 사이버테러의 유형과 그 피해범위가 확대되고 있는 시점에서 전문가 양성을 책임지고 담당할 정부부처와 유관기관을 명확히 하는 법률을 제정할 필요가 있다[3][23].

둘째, 산·관·학이 공동으로 대학 및 전문교육기관에 사이버테러에 대응할 수 있는 전문가를 육성할 수 있도록 교육비 지원이나 장학제도를 마련하여 우수한 인재를 수급하는 방안이 고려될 수 있다[9]. 현재, 고려대학교 및 아주대학교에서 사이버보안 전문가(군 장교)를 육성하기 위한 학과를 개설하여 국가로부터 교육비 지원 및 장학혜택을 받고 있는 점은 전문가 인력 수급 확보에 긍정적이다. 따라서 추후 많은 대학과 전문교육기관에 사이버안전 및 안보관련 전공 및 학과 개설과 함께 국가정책적으로 다양한 지원방안이 고려될 필요가 있다.

마지막으로, 보안전문가로도 표현할 수 있는 화이트 해커를 국가차원에서 관리하는 방안을 들 수 있다. 화이트 해커는 모의 해킹(penetration testing)이나 취약점 점검 등의 해킹 기법을 사용하는 전문적인 보안전문가이다. 따라서, 국제적 대회나 국가에서 실시되고 있는 여러 대회에서 입상 경력이 있는 이들을 국가차원에서 관리하고 이들에게 애국심 및 당위성을 부여하여 국가 안보에 기여시키는 방안이 필요하다. 물론, 이 경우 허가받은 범위를 벗어나 해킹행위를 하게 될 경우를 대비하여, 법적 책임 역시 마련되어야 할 것이다[10].

4. 결 론

기존의 사이버테러와 관련된 대부분의 선행연구에서는 한국에서 사이버테러 대응체제 구축방안으로 미국 국토안보부와 같은 기능을 총괄 및 조정하고, 각 기능을 통합할 수 있는 컨트롤타워의 설치, 그리고 위기상황에서 신속하고 효과적으로 대응 할 수 있도록 정보 수집, 전파의 체계 구축, 단일화된 법률의 제정 및 개정과 사이버테러 대응 시스템의 체계적인 정비, 인터넷 등 네트워크의 견고성 및 방어력 고취, 국가기반시설별 보호프로그램 마련, 국민들의 인식 전환 등을 제시하고 있다[17][20][12][11]. 덧붙여 세계적으로도 사이버테러로부터 안전을 확보하기 위한 사이버테러 방어시스템의 구축과 정보시스템의 보안 대책을 강구하기 위한 국가간 협력체계의 구축도 진행 중이다. 우리나라도 급증하는 사이버테러의 위험에 적극적으로 대처하기 위해서 더욱 심도깊은 논의와 준비가 절실한 시점이다.

이 연구에서는 우리나라 사이버테러 방지를 위한 효과적인 대응방안에 대해서 논의해 보았다. 사이버안보 및 사이버테러방지를 위한 역량강화를 위해서 통합적인 체제로의 재구성을 제안을 하였으며, 이는 해당

업무를 담당하는 기관의 역할과 책임에 대해서 명확한 법적근거규정을 마련하는 것부터 시작되어야 할 것이다. 우리나라에서 발생되고 있는 사이버테러를 방지하고 대응역량을 강화하여 사이버안보를 확보하기 위한 체제정비를 위한 요청은 더 이상 늦추어서는 안 될 문제이다. 사이버테러방지법의 필요성은 관련 선행연구를 통해서도 이미 지속적으로 제기되어 왔으며, 2013년 상반기부터 국회에서 '국가 사이버테러방지에 관한 법률안', '국가 사이버안전 관리에 관한 법률안', '정보통신기반 보호법 일부개정법률안' 등이 발의되어 관련 법률의 정비를 위한 개선노력이 시도되어 오고 있다. 앞서 논의한 사이버테러방지법(가칭)의 쟁점과 관련된 사항에 대해서는 아직도 많은 논쟁이 진행 중이지만, 궁극적으로 우리나라 사이버안보의 중요성과 현재 사이버테러대응의 문제점을 제대로 정비하기 위해서는 입법화가 불가피하며, 각계각층의 의견수렴과 함께 국회에서 논의를 더욱 활발히 진행해나가야 할 것이다.

이 연구는 현재까지 진행되어 온 사이버안전 및 테러 방지와 관련된 주요한 쟁점과 선행연구의 내용분석을 바탕으로 사이버테러 방지를 위한 대응방안을 제안하였다는 점에서 학술적, 정책적으로 기여를 하였다. 그럼에도 불구하고, 이 연구는 사이버안전 및 테러와 관련된 주요한 쟁점에 대한 해당 분야 실무자의 의견이나 인식을 통한 실증연구나 또는 외국의 사례분석을 통한 효과성 검증으로 통한 실증연구결과를 제시하지 못하였다는 점이 한계로 남으며, 향후 관련 연구에서는 이러한 연구들이 진행되어 사이버안전 및 테러분야에서 보다 다양한 많은 논의가 진행되기를 기대한다.

참고문헌

[1] 강석구, 이원상, "사이버범죄 관련 법령정비 방안", 한국형사정책연구원 연구총서, 2014.

[2] 곽병선, "사이버테러 대응을 위한 법체계 검토", 법학연구, 제59권, pp. 1-24, 2015.

[3] 권문택, "사이버테러정보전 전문인력 양성 및 관리 방향에 대한 연구", 융합보안 논문지, 제5권 제3호, pp. 43-57, 2005.

[4] 권한용, "사이버테러에 대한 국제적 대응방안과 한국에의 시사점", 동아법학, 제65호, pp. 649-675, 2014.

[5] 권현준, "사이버보안법제 선진화 방안 연구", 한국방송통신위원회 연구보고서, 2011.

[6] 김도승, "사이버위기 대응을 위한 법적 과제: 미국의 사이버위기 대응체계 현황과 시사점을 중심으로", 방송통신정책, 제21권 제17호, pp. 21-56, 2009.

[7] 김지현, "헌법의 관점에서 본 사이버 보안컨트롤타워 제도 구축에 관한 고찰", 보안공학연구논문지, 제11권 제1호, pp. 25-40, 2014.

[8] 김태계, "사이버테러 범죄 대응에 관한 제도적 문제점과 대책", 법과 정책연구, 제14권 제3호, pp. 1337-1381, 2014.

[9] 문재명, "국가안보를 위한 사이버테러 대응방안 연구", 한국테러학회보, 제4권 제2호, PP. 5-32, 2011.

[10] 박대우, "국가사이버보안정책에서 해킹에 대한 소고", 정보보호학회지, 제21권 제6호, pp. 23-40, 2011.

[11] 박동균, "북한의 사이버 테러공격 가능성 및 대비전략", 국가위기관리학회보, 제1권, pp. 53-66, 2009.

[12] 박동균, 김태민, "미국 사이버테러 대응 시스템의 특징 및 함의", 한국위기관리논집, 제8권 제6호, pp. 31-49, 2015.

[13] 변찬호, 김은정, "북한 테러범죄의 변화양상에 따른 대응방안: 김정일 정권 이후 고위층 권력갈등을 중심으로", 제39호, pp. 185-215, 2014.

[14] 심우민, "최근 전산망 마비사태와 사이버 테러 대응체계 개선방안", 이슈와 논점, 제640호, 2013.

[15] 오길영, "사이버테러 대응체제의 문제점과 개선방향", 민주법학, 제54호, pp. 461-484, 2014.

[16] 윤민우, "새로운 안보환경을 둘러싼 사이버 테러의 위협과 대응방안", 한국경호경비학회지, 제40호, pp. 109-145, 2014.

[17] 윤해성, 윤민우, J. Freilichm, S. Chermak and R. G. Morris, "사이버 테러의 동향과 대응 방안에 관한 연구", 한국형사정책연구원 연구총서, 2012.

[18] 이대성, “한국의 안보위협요인 분석을 통한 안보정책의 재평가와 제언”, 한국테러학회보, 제8권 제1호, pp. 99-114. 2015.
[19] 정완, “한・미 사이버보안 법제 동향에 관한 고찰”, 경희법학, 제48권 제3호, pp. 213-242, 2013.
[20] 주성빈, “사이버 테러리즘에 대한 억지력 모색”, 한국안보정책학회・국가안전정책학회 학술세미나 발표자료집, 2015.
[21] 차성민, “ICT정부조직 비교연구”, 한국비교정부학보, 제16권 제3호, pp. 187-208, 2012.
[22] 한국인터넷진흥원, 2010, “침해사고대응팀(CERT) 구축/운영 안내서”, KISA 안내・해설 제 2010-13호.
[23] 한희원, “사이버 안보에 대한 국가정보기구의 책무와 방향성에 대한 고찰”, 한국경호경비학회지, 제39호, PP. 319-353, 2014.
[24] Ballard, J. D., Hornik, J. G., & McKenzie, D. (2002). Technological Facilitation of Terrorism Definitional, Legal, and Policy Issues. American Behavioral Scientist, 45(6), 989-1016.
[25] Dogrul, M., Aslan, A., & Celik, E. (2011, June). Developing an international cooperation on cyber defense and deterrence against Cyber terrorism. In Cyber conflict (ICCC), 2011 3rd international conference on (pp. 1-15). IEEE.
[26] Lewis, J. A. (2002). Assessing the risks of cyber terrorism, cyber war and other cyber threats. Washington, DC: Center for Strategic & International Studies.
[27] 경찰청 국회정보공개 (http://www.police.go.kr/assembly/).

[저 자 소 개]

성 용 은 (Yong-Eun Sung)

동국대학교 경찰행정학과
(경찰학/범죄학 박사)
Rutgers University-Newark
(Criminal Justice 박사수료)
극동대학교 경찰행정학과 교수

E-mail: ysung@kdu.ac.kr

윤 병 훈 (Byung-Hoon Youn)

동국대학교 경찰행정학과
(경찰학 석사)
동국대학교 경찰행정학과
(경찰학 박사)
경동대학교 경찰학과 교수

E-mail: hoony0710@kduniv.ac.kr